

אלגברה ב' 2 – הרצאה 4

02.03.11

מהשיעור הקודם נותר לנו לזהות שאם R תחום פריקות, אז $c \in R$ אז $c \cdot \gcd(a_1, \dots, a_n) = \gcd(ca_1, \dots, ca_n)$.
אכן, אם $c = 0$ אז זה ברור. בה"כ $a_1, \dots, a_n$ שונים מ-0 (אפשר לזרוק את האפסים כי כל מספר מחלק את 0). נכתוב עבור $j = 1, 2, \dots, n$:

$$a_j = u_j \prod_{i \in I} p_i^{n_{ij}}$$

$$c = v \prod_{i \in I} p_i^{m_i}$$

כעת ניתן לכתוב:

$$ca_j = vu_j = \prod_{i \in I} p_i^{n_{ij} + m_i}$$

הוכחנו כי:

$$d = \prod_{i \in I} p_i^{\min_j(n_{ij})} \in \gcd(a_1, \dots, a_n)$$

לכן,

$$cd = v \prod_{i \in I} p_i^{m_i + \min_j(n_{ij})} = \underbrace{v \prod_{i \in I} p_i^{\min_j(m_i + n_{ij})}}_{\in \gcd(ca_1, \dots, ca_n)}$$

ולכן,

$$v \prod_{i \in I} p_i^{\min_j(m_i + n_{ij})} \in c \gcd(a_1, \dots, a_n)$$

מעכשיו R הוא תחום פריקות.

הגדרה. $f = \sum_{i=0}^{\infty} a_i x^i \in R[x]$ נקרא פרימיטיבי אם $1 \in \gcd(a_0, a_1, \dots)$.

כלומר, $f \neq 0$ ולכל p_i ממערכת הנציגים יש מקדם a_j כך ש- $a_j \nmid a_i$. לכל $p \in R$ אי פריק, יש a_i כך ש- $p \nmid a_i$.

הערה. אם f פרימיטיבי $c \in R^*$ אז cf פרימיטיבי.

למה. אם $f, g \in R[x]$ פרימיטיביים אז fg פרימיטיבי.

הוכחה. נניח $f = \sum_{i=0}^{\infty} a_i x^i$, $g = \sum_{j=0}^{\infty} b_j x^j$ אז $fg = \sum_{k=0}^{\infty} (\sum_{i+j=k} a_i b_j) x^k$ יכול להיות שיש הרבה כאלה אז ניקח $p \in R$ אי פריק. אז יש i, j כך ש- $a_i \nmid p$, $b_j \nmid p$. יכול להיות שיש הרבה כאלה אז ניקח i, j קטנים ביותר. אז המקדם של x^{i+j} ב- fg הוא

$$c_k = \underbrace{(a_0 b_{i+j} + \dots + a_{i-1} b_{j+1})}_{\text{כפולה של } p} + a_i b_j + \underbrace{(a_{i+1} b_{j-1} + \dots + a_{i+j} b_0)}_{\text{כפולה של } p}$$

אז $a_i b_j$ אינו מתחלק ב- p כי p אי פריק ולכן ראשוני. לכן $p \nmid c_k$ ולכן fg פרימיטיבי. $\square$

למה. יהי F ההרחבה של R לשדה. ניקח פולינום $f = \sum_{i=0}^{\infty} a_i x^i \in F[x]$

1. יש $c \in F^*$ ויש $p \in R[x]$ פרימיטיבי כך ש- $f = cp$.

2. אם גם $f = c'p'$ כאשר $c' \in F^*$ ו- $p' \in R[x]$ אז $\frac{c'}{c} \in R^*$.

3. אם $f \in R[x]$ ויהי c כמו בסעיף הראשון אז ביתר דיוק $c \in \gcd(a_0, a_1, \dots)$.

הוכחה.

1. בה"כ נניח כי $f \in R[x]$ אחרת נכפיל את f באיזה $a \in R$ $a \neq 0$ כך ש- $af \in R[x]$. יהי $c \in \gcd(a_0, a_1, \dots)$ אז $c | a_0, a_1, \dots$ ואז $\frac{a_0}{c}, \frac{a_1}{c}, \dots \in R$. מדוע? ברור כי הוכיח! אם $d \in \gcd(\frac{a_0}{c}, \frac{a_1}{c}, \dots)$ אז $cd \in \gcd(a_0, a_1, \dots)$ אבל גם $c \in \gcd(a_0, a_1, \dots)$ ולכן $(c) = (cd)$, כלומר $cd = cu$ כאשר u הפיך, כלומר $d = u$ הפיך.

נגדיר $p \in R[x]$ $p = \frac{a_0}{c} + \frac{a_1}{c}x + \frac{a_2}{c}x^2 + \dots$ פרימיטיבי וכמובן $cp = f$.

2. נניח $cp = f = c'p'$ צ"ל ש- $\frac{c'}{c} \in R^*$. נכפיל את שני האגפים באיבר של R נוכל להניח בה"כ ש- $c, c' \in R$.

$$\begin{aligned} &= \gcd(cp \text{ של המקדמים של } p) = \gcd(c \cdot 1 \in c \gcd(p \text{ של המקדמים של } p)) \\ &= \gcd(c'p' \text{ של המקדמים של } p') = c' \gcd(p' \text{ של המקדמים של } p') \ni c' \cdot 1 = c' \end{aligned}$$

מכאן, $(c') = (c)$ כלומר $c' = cu$ כאשר $u \in R^*$.

3. הוכחנו כבר בסעיף הראשון שאפשר לקחת $c \in R$ ואפילו $c \in \gcd(a_0, a_1, \dots)$ וזה עובד. אולי יש c אחר שגם מקיים? נניח $f = c'p'$, כאשר $c' \in R$ ו- $p' \in R[x]$ פרימיטיבי אז ל לפי הסעיף השני $c' = cu$ כאשר $u \in R^*$. לכן $c' \in R$ ו- $c' \in \gcd(a_0, a_1, \dots)$.

$\square$

למה.

1. $(R[x])^* = R^*$.

2. יהי $a \in R$ אז a אי פריק ב- $R[x]$ אם ורק אם a אי פריק ב- R .

3. יהי $f \in R[x]$ מפעלה $1 \leq \deg f$ אי פריק ב- $R[x]$ אם ורק אם f פרימיטיבי ואי פריק ב- $F[x]$.

נרה קודם טענת עזר:

טענה. יהי $a \in R, a \neq 0$ וניקח $f_1, f_2 \in R[x]$ כך ש- $a = f_1 f_2$ אז $f_1, f_2 \in R \setminus \{0\}$.
הוכחה. אכן, $f_1 f_2 \neq 0$ לכן $f_1 \neq 0, f_2 \neq 0$ לכן $\deg f_1, \deg f_2 \geq 0$ אבל $\deg f_1 + \deg f_2 = \deg a = 0$
 $\square$ $f_1, f_2 \in R \setminus \{0\}$ כלומר $\deg f_1 = \deg f_2 = 0$, לכן $\deg f_2 = \deg a = 0$

הוכחה. למה

1. נציב $a = 1$ בטענת עז. נקבל כי $(R[x])^* \subseteq R^*$ ההיפך תמיד נכון ולכן $(R[x])^* = R^*$.

2. נניח $a = f_1 f_2$ לפי טענת העזר בהכרח $f_1, f_2 \in R$ ומתקיים $f_i \in R^* \Leftrightarrow f_i \in R$ ולפי ההגדרות של אי פריקות נקבל את הנדרש.

3. נניח $f \in R[x]$ אי פריק נראה כי f פרימיטיבי. לפי הלמה הקודמת $f = c \cdot p$ כאשר $c \in R, c \neq 0, p$ פרימיטיבי.

$\deg p \geq 1$ ולכן $\deg g \geq 1$. בפרט p אינו פריק $(R[x])^* = R^*$ (כי $p \notin R^*$). אי פריק f ב- $R[x]$ ולכן c הפיך ב- $R[x]$, כלומר $c \in (R[x])^* = R^*$.

p פרימיטיבי ולכן גם f פרימיטיבי. כעת, נראה כי f אי פריק ב- $F[x]$: נניח $f = f_1 \cdot f_2$, $f_i \in F[x]$. לפי הלמה, $f_i = c_i p_i$, $c_i \in F^*, p_i \in R[x]$ פרימיטיבי. כעת, $f = [c_1 \cdot c_2][p_1 \cdot p_2]$ כאשר $p_1 \cdot p_2$ פרימיטיבי, $c_1 \cdot c_2 \in F^*$ ולפי הלמה $c_1 \cdot c_2 \in R$. f אי פריק ב- $R[x]$ אינו הפיך ב- $R[x]$ (כי $\deg f \geq 1$) $\deg(p_1 \cdot p_2) = \deg f \geq 1$ לכן גם $c_1 \cdot c_2 \in R^*$. $c_1 \cdot c_2 \in R^*$ לכן $(c_1 c_2)^{-1} f = p_1 \cdot p_2$ אי פריק ב- $R[x]$ לכן בה"כ $p_1 \in (R[x])^* = R^*$ (אחד מהם צריך להיות הפיך). לכן $p_1 \in R^* \subseteq F^*$ ואז $f_1 = c_1 p_1 \in F^* \subseteq (F[x])^*$.

לכן, f_1 הפיך ולכן f אי פריק ב- $F[x]$.

כעת נוכיח את הצד השני. נניח כי f פרימיטיבי ואי פריק ב- $F[x]$. נראה כי הוא אי פריק ב- $R[x]$. נניח כי $f = f_1 \cdot f_2$ כאשר $f_1, f_2 \in R[x]$. לפי הנתון, בה"כ $f_1 \in (F[x])^* = F^*$. מתקיים $F^* = (F[x])^*$ ולכן $f_1 \in F^*$. אולם $f_1 \in R[x]$ ולכן $f_1 \in R$. $0 \neq f_1 \in R$ לכן f_1 הפיך ב- $R[x]$ לכן f_1 מחלק את המקדמים של f ב- R . אולם f פרימיטיבי ולכן $f_1 \in R^*$ ולכן $f_1 \in (R[x])^*$ ולכן f אי פריק.

$\square$

משפט. אם R תחום פריקות אזי $R[x]$ תחום פריקות.

הוכחה. ניקח מערכת מייצגים $\{r_i\}_{i \in I}$ של איברים אי פריקים ב- R . תהי $\{f_j\}_{j \in J}$ קבוצת הפולינומים האי פריקים המתוקנים ב- $F[x]$ ממעלה $1 \leq$. לכל $j \in J$ יש $c_j \in F^*$ ו- $p_j \in R[x]$ פרימיטיבי כך ש- $f_j = c_j p_j$ נקבע אותם (כי הם לא יחידים).

טענה. $\Gamma := \{r_i\}_{i \in I} \cup \{p_j\}_{j \in J}$ מערכת מייצגים של איברים אי פריקים ב- $R[x]$.

הוכחה. אכן, כל איברי Γ הם אי פריקים ב- $R[x]$ (אי פריק לכן גם $c_j^{-1} f_j = p_j$ אי פריק ב- $F[x]$).

נוכיח כי לכל f אי פריק יש $g \in \Gamma$ יחיד כך ש- $f = u \cdot g$ עבור איזשהו $u \in (R[x])^* = R^*$. אכן אם $\deg f = 0$ כלומר $f \in R$ יש r_i יחיד כך ש- $f = u \cdot r_i$, $u \in R^*$ (וכמובן $f \neq u \cdot p_j$ עבור אף p_j , $u \in R^*$ כי $\deg f = 0 < \deg p_j$). אם $\deg f \geq 1$ אז אי פריק ב- $F[x]$ ולכן יש $j \in J$ יחיד כך ש- $f = c \cdot f_j$ עבור איזשהו $c \in F^*$.

לכן $f = c \cdot c_j \cdot p_j$ ועבור $u = c \cdot c_j \in F^*$ מתקיים $f = u \cdot p_j$ (כי p_j מתוקן), ואפילו $u \in R^*$ כי f אי פריק (תרגיל לבית הוא לבדוק שהוא יחיד). $\square$

יהי $f \in R[x]$, $f \neq 0$. כיוון ש- $F[x]$ תחום פריקות (מקסנה מהשיעור הקודם) אז לכל $j \in J$ יש $m_j > 0$ (כמעט כולם אפס) כך שמתקיים $f = c \cdot \prod_{j \in J} f_j^{m_j}$ עבור איזשהו $c \in F^*$.
לכן,

$$f = c \cdot \underbrace{\prod_{j \in J} c_j^{m_j}}_{:= \tilde{c}} \cdot \underbrace{\prod_{j \in J} p_j^{m_j}}_{\tilde{p}}$$

$\tilde{p}$ פרימיטיבית (כמכפלת פרימיטיביות) ולכן אנו מקבלים $\tilde{c} \in R$ (כי $f \in R[x]$) כמו כן $\tilde{c} \neq 0$ ולכן נוכל $i \in I$ $n_i \geq 0$ (כמעט כולם 0) כך ש- $\tilde{c} = u \prod_{i \in I} r_i^{n_i}$ עבור $u \in R^*$.
ולכן נקבל $f = u \prod_{i \in I} r_i^{n_i} \prod_{j \in J} p_j^{m_j}$ כאשר $u \in R^*$ ולכן $R[x]$ תחום פריקות. $\square$

מסקנה. אם R תחום פריקות אזי גם $R[x_1, \dots, x_n]$ תחום פריקות.

$\square$ הוכחה. באינדוקציה על n . כי מתקיים $R[x_1, \dots, x_n] = R[x_1, \dots, x_{n-1}][x_n]$